TR No. AMSEL-IE-SP-98163
September 1998

# C2 Protect Tool Kit Implementation Guidance for Windows NT Systems

# ENCLOSURE 2

## TABLE OF CONTENTS

**Paragraph** **Page**

## TABLE OF CONTENTS

**Paragraph** **Page**

## FIGURES

TR No. AMSEL-IE- SP-98163
September 1998

# C2 Protect Tool Kit Implementation Guidance for Windows NT Systems

## 1.0 Introduction

1.1 Purpose.
The purpose of this document is to aid Windows NT administrators in the acquisition, installation, configuration and usage of the Command and Control (C2) Protect Tools that are recommended for use on Windows NT systems. Currently, the Security Profile Inspector for Windows NT (SPI-NT) is the only recommended C2 Protect Tools for Windows NT systems. This document is intended to provide sufficient information and instruction that will enable the administrator to easily and confidently load and operate SPI-NT, and thus obtain a strengthened system security posture.

1.2 Scope.
This document only applies to Windows NT operating systems and is intended solely as guidance to aid administrators in performing the tasks associated with acquiring, installing, configuring, and operating the C2 Protect Tools for Windows NT. System administrators are ultimately responsible for the proper configuration and usage of the C2 Protect Tools.

1.3 Background.
The C2 Protect Tool Kit was introduced through a Director of Information Systems for Command, Control, Communications, and Computers (DISC4) memorandum, dated 11 April 1996. The memorandum states,

> "The Army C2 Protect Program Implementation Plan and AR 380-19 (Information Systems Security) requires that all prudent measures be taken to protect our systems; the information they manage, produce, store and distribute. The Army C2 Protect library defines the need for the acquisition, integration and implementation of C2 Protect software applications into information systems by system administrators and managers. As a result of recent intrusions and penetrations of Army systems by unauthorized elements, network managers in all environments are directed to acquire C2 Protect Tools for use in the security management of their systems. System developers are advised to integrate GFE security protection, detection and misuse tools during their system design and build phases. These tools will aid in this effort."

This initial C2 Protect Tool Kit memorandum identified three UNIX security tools as mandated security tools to be used on all UNIX operating system platforms. These were the Security Profile Inspector (SPI), TCP Wrapper and Simple Watcher (SWATCH). As time has progressed, however, support for SPI has been redirected to an improved application called Security Profile Inspector for Networks (SPI-NET). Additionally, Security Profile Inspector for Windows NT (SPI-NT) was introduced to aid in the protection of Windows NT based systems.

## 2.0 General Information

2.1 C2 Protect Tool Kit Information.
From the U.S. Army perspective, two organizations provide direct support and assistance related to C2 Protect Tools: the Defense Information Systems Activity (DISA) Automated Systems Security Incident Support Team (ASSIST) and the Army Computer Emergency Response Team (ACERT). The ASSIST has the following mission statement:

> "The Automated Systems Security Incident Support Team (ASSIST) is the INFOSEC Incident Response Support to the Defense Information Infrastructure (DII) Community in Support of Information Assurance.
>
> Our Goal is to Identify, Analyze, Assess and Resolve all INFOSEC Vulnerabilities and Exploitation in the DII in Support of the Defense Information Systems Agency's (DISA) Information Assurance Mission."

The mission statement for the ACERT is as follows:

> "The Army Computer Emergency Response Team (ACERT) conducts command and control protect operations in support of the Army to ensure the availability, integrity, and confidentiality of the information and information systems used in planning, directing, coordinating, and controlling forces in the accomplishment of the mission across the full spectrum of support to military operations."

Both ASSIST and ACERT provide a variety of computer security services and resources. Most important among these services and resources are security bulletins, frequently asked questions (FAQs), links to vendor security patches, incident reporting information, and access to the C2 Protect Tool Kit.

An additional Governmental agency of importance is the Lawrence Livermore National Laboratories (LLNL). LLNL is the developer of the SPI portions of the C2 Protect Tool Kits, including SPI and SPI-NET for UNIX and SPI-NT for Windows NT systems. All SPI components are owned by the U.S. Government and are not public domain software.

2.2 Securing Windows NT.
The scope of this document does not encompass all of the tasks and steps required to fully secure Windows NT. The SPI for NT tools will highlight many of the security problems associated with Windows NT but it cannot be assumed that any single tool will totally secure the Windows NT operating system. It is advised that SPI for NT be used in conjunction with checklists or guides available from various sources to more fully secure a platform running Windows NT. The SANS Institute offers one of the best guides for securing Windows NT, titled "Windows NT Security: Step by Step." Information on this booklet can be obtained by email info@sans.org or by telephone (301) 951-0102.

### 2.3 Document Legend.

To aid the reader, different fonts will be used to differentiate between textual guidance, keyboard actions, and computer configuration files.

All text printed using the Arial font is Microsoft (MS) WinNT command text, designed to be typed at the command line.  This font is also used to indicate menu paths and the like.

All text printed using the Courier New font represents MS WinNT system file readings, designed to show portions of configuration files or other text information located on the system.  This font is also used to identify buttons and window areas of a screen.

## 3.0 Security Profile Inspector for Windows NT (SPI-NT)

### 3.1 Overview.

SPI for NT is a host-based vulnerability and intrusion detection tool for Microsoft Windows NT 4.0 environments. Among its features, SPI-NT checks for binary file modifications, vulnerable versions, weak passwords, and common misconfigurations. Along with the other SPI components, SPI-NT was developed by Lawrence Livermore National Laboratories (LLNL) and is freely available to all U.S. Government Federal entities and contractors directly supporting the Department of Defense (DoD).

### 3.2 Introduction to the Tools.

SPI-NT employs five security tools, four of which are provided by SPI-NT. The four tools included with SPI-NT are the Binary Authentication Tool (BAT), Change Detection Test (CDT), Password Security Inspector (PSI), and Quick System Profile (QSP). An added Virus Detection Tool (VDT) can be utilized if provided by the user.

#### 3.2.1 Binary Authentication Tool (BAT).

The BAT is a utility that checks the integrity and version of the currently installed Windows NT 4.0 operating system.

#### 3.2.2 Change Detection Test (CDT).

The CDT can act as an intrusion detection tool in that it can be used to detect changes made in the file system.

#### 3.2.3 Password Security Inspector (PSI).

The PSI attempts to discover weak passwords in local user accounts.

#### 3.2.4 Quick System Profile (QSP).

The QSP performs a variety of checks to detect improper configuration settings that can impact security.

### 3.3 Acquisition.

The C2 Protect Tools, including SPI-NT, are available for download from several file transfer protocol (FTP) areas and web sites. The latest release of SPI-NT is version 1.4 which was released 10 March 1998. The download file is called “spint-1.4.exe” and is a self-extracting installer. It is advised that users also download the SPI-NT README file. The following is a list of sites from which an authorized user can acquire SPI-NT:

| | | |
|---|---|---|
| ASSIST: | WWW | www.assist.mil |
| | FTP | ftp.assist.mil/pub/tools |
| ACERT | WWW | www.acert.belvoir.army.mil/tools.html |
| | FTP | ftp.acert.belvoir.army.mil/pub/nt.toolbox/SPI/ |

| | | |
|---|---|---|
| LLNL | WWW | ciac.llnl.gov/cstc/cstc.html |

For the ACERT and ASSIST, downloads can only be performed from a DNS-registered ".mil" location. A password is required to download from LLNL. The download password can be requested from LLNL via an on-line registration form. The ACERT, ASSIST, and LLNL use these access control methods to limit the distribution of SPI-NT to authorized users. All U.S. Government Federal entities and directly supporting contractors are authorized to obtain and utilize SPI-NT.

In addition to the SPI-NT software, the operator must acquire the installation password for SPI-NT prior to starting the installation process. The installation password is the same for all copies of the same version regardless of the location from which it is obtained. For those who obtain SPI-NT from LLNL, the message from LLNL that contains the download password will also contain the installation password. The installation password can also be obtained from ASSIST or ACERT telephonically by contacting the following:

| | | | |
|---|---|---|---|
| ASSIST | 1-800-357-4231 | or | DSN 327-4700 |
| ACERT | 1-888-203-6332 | or | DSN 235-1113/1922 |

A DSN phone is required since ASSIST/ACERT will call back to give out the installation password and will only return calls to DSN phone numbers.

### 3.4 Installation.

The following paragraphs address the procedures necessary to properly install and set-up SPI-NT for operations. Prior to beginning the installation, it is highly advised that the operator review the SPI-NT README file.

### 3.4.1 Removing Prior Versions.

Prior to installing a new version of SPI for NT, any old versions of SPI-NT must be removed. The old version can be removed using the Install/Uninstall page within Control Panel -> Add/Remove Programs utility. To remove SPI-NT from the Install/Uninstall page, select the "SPI for NT" program and then press `Add/Remove`. A confirmation window will appear to confirm the program removal. The removal process will not affect existing reports; however, the installation of the new version of SPI-NT may use a different directory area causing the old reports to be orphaned unless relocated. For additional information refer to "Process 1: Removing the SPI for NT installation" in the README file.

### 3.4.2 SPI-NT Installation.

The actual installation of the SPI-NT program is simple and straight forward. To begin the installation, go to the directory where the SPI-NT file is located and execute the SPI-NT self extractor.

spint_1.4.exe

The installation process will proceed through a series of eight major windows.

(1) InstallShield SPI for NT program window.

(2) Installation Password. At the start of the installation process, the operator will be prompted to enter the installation password that was obtained. If the correct password is entered, the Next button will become accessible. This is the only indication of a correct password entry; no indication is given if an incorrect password is entered.

(3) Installation Directory. The installation process first unpacks the various installation files. The SPI-NT installation files are temporary and can be unpacked into any location. If the desired directory does not exist, the installer will create the directory prior to unpacking the installation files. Note that these installation files are not automatically removed at the end of the installation process. The files and associated directory can be deleted at the operator's convenience after the installation process is complete.

(4) SPI for NT Welcome window.

(5) Software License Agreement. Select "Yes" to agree to the distribution and usage licensing agreement.

(6) Information window.

(7) Destination Location. The operator will also be given the option to select the directory in which the SPI-NT executable will reside. The default directory is C:\Program Files\Lawrence Livermore National Laboratory\SPI for NT 1.4.

(8) Select Program Folder. The operator has the option to select the program folder in which the SPI for NT link will be placed. By default, it will be placed in its own program folder.

*Installation Complete !!*

3.4.3 SPI-NT Administrator Set-up.

Three tasks are needed to properly establish an SPI-NT Administrator. First, a user must be created to act as the SPI-NT Administrator. Secondly, the SPI-NT Administrator must be assigned the right to "Act as part of the operating system." Lastly, the registry must be edited to allow the SPI-NT Administer "Full Access" control of the local SAM.

(1) Creating SPI-NT Administrator. A new user can be created with the User Manager which is accessed by Programs -> Administrative Tools -> User Manager. The New User creation screen is accessed by User -> New User. The operator will be asked to

supply a Username, Full Name, Description, and Password. The user name can be any unique identifier; it does not have to be “SPI-NT Administrator.” To properly administer SPI-NT, the SPI-NT Administrator must be a member of both the Users and Administrators groups. This can be checked and modified as needed by selecting the Groups button, and adding the appropriate Groups as required to the Members of: area. Press OK, as required, to finalize the user creation. This process is described in the SPI for NT README file as “Process 2: Adding a new user to administer SPI for NT.”

(2) Setting the SPI-NT Administrator Rights and Permissions. The SPI-NT Administrator must be given the right to “Act as part of the operating system” to properly operate SPI for NT. First highlight the SPI-NT Administrator in the User Manager screen (Programs -> Administrative Tools -> User Manager), then select Policies -> User Rights to display the User Rights Policy screen. At this screen, check the box for “Show Advanced User Rights.” With this item checked, use the pull-down selector on the Right list to select “Act as part of the operating system.” To grant the “Act as part of the operating system” right to the SPI-NT Administrator, select the Add button followed by the Show Users button to display a screen that allows the operator to add names to the list of names to be granted that right. From the list of names identify the SPI-NT Administrator by either double-clicking the name or selecting the name and pressing the Add button. The Add Names window should show the user or name that will be assigned this right. Select OK to confirm and continue as required. This process is described in the SPI for NT README file as “Process 3: Act As Part of the OS.”

(3) Modify the Registry. Modifications to the Windows NT registry are performed by using the NT Registry Tool (C:\WINNT\system32\regedt32.exe). With the tool started, open the HKEY_LOCAL_MACHINE window and highlight the SAM folder. With the SAM folder highlighted, pull down the “Security” menu and choose “Permissions…” to activate the Registry Key Permissions window. If the SPI-NT Administer is listed, highlight that user account and change the “Type of Access” to Full Control. If the SPI-NT Administer is not listed, add the user account to the list with the Add button. At this same time the Type of Access can be set to Full Control. Note that the Show Users button may be needed to display all user accounts. This process is described in the SPI for NT README file as “Process 3: Act As Part of the OS.”

### 3.5 Basic Operations.

This section will cover the SPI-NT menu, how to launch the tools and how to access the reports.

### 3.5.1 SPI for NT Menu.

The SPI-NT Main Menu consists of four primary pull-down menus: File, Jobs, Reports, and Help. Figure 3-1 shows the SPI for NT main menu with the Jobs area accessed. The following is a list of menu items associated with the SPI for NT menu system:

File. Use the File menu to exit the SPI for NT program.

File -> Exit

Jobs. Use the Jobs menu to launch a tool or set the default level.

Jobs -> Binary Authentication Tool
Jobs -> Change Detection Test
Jobs -> Password Security Inspector
Jobs -> Quick System Profile
Jobs -> Virus Detector
Jobs -> Default Level

Reports. Use the Manage Reports item to view, print, archive, or delete reports.

Reports -> Manage Reports

Help. This menu area provides limited information about SPI for NT and information about the program and developers.

Help -> Contents
Help -> About SPI for NT
Help -> About CSTC
Help -> Acknowledgments

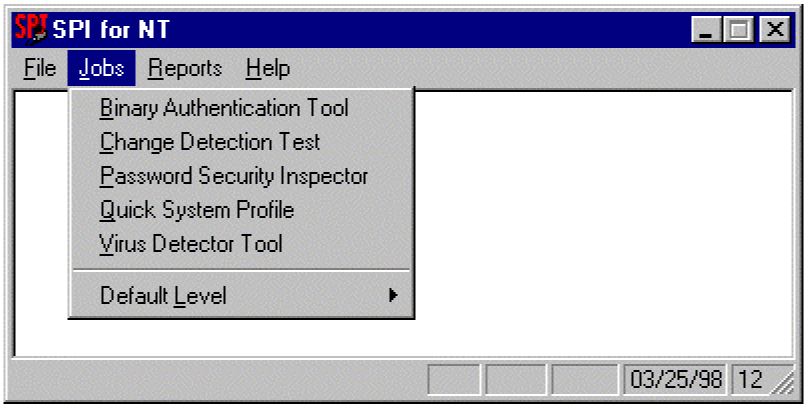
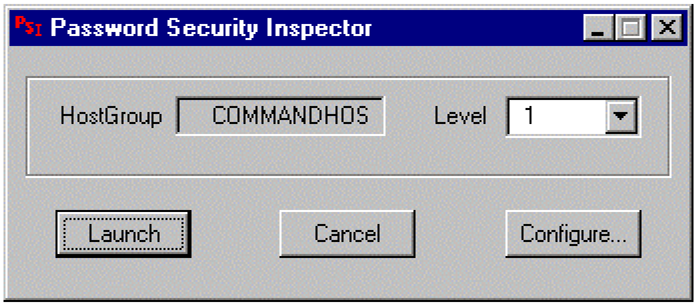


**Figure 3-1. SPI for NT Main Menu**

3.5.2 Jobs: Launching the Tools.
To launch a specific SPI-NT tool, select the desired tool from the Jobs menu listing. When the desired tool is selected (double click), a window arises that allows the operator to adjust the Level associated with the tool and either configure or launch the tool. The Level aids in defining the severity or depth of the actions performed by the tool and is discussed as part of the configuration details. Press the `Launch` button to begin using the tool. A progress bar will be

displayed to show the status of the tool operations. Each time a job is started, an entry representing that job will appear in the Report Manager screen. Figure 3-2 shows a sample job window for the Password Security Inspector.



HostGroup COMMANDHOS

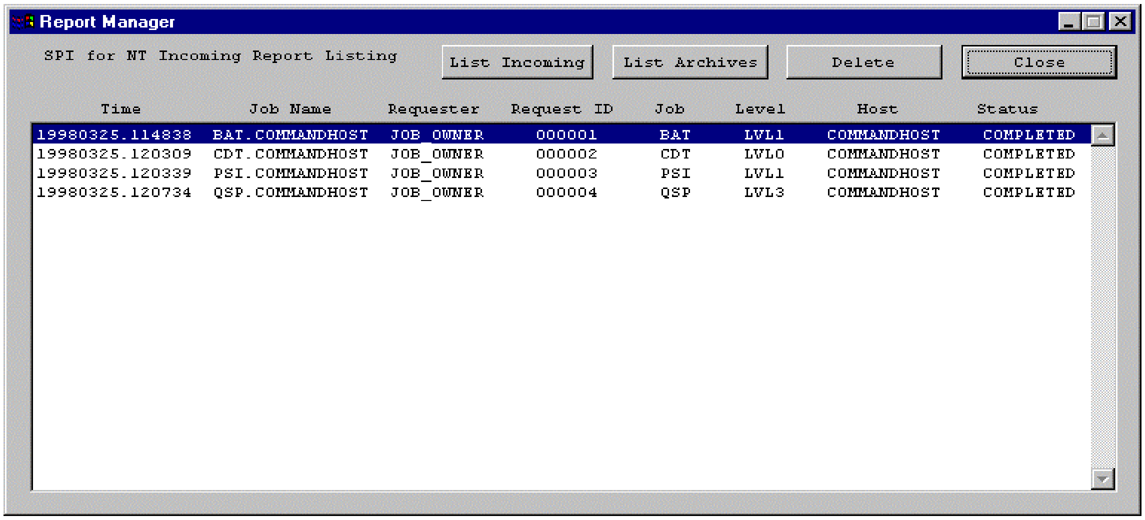
Level 1

**Figure 3-2. Job Launch Window**

Currently, SPI for NT has no mechanism to schedule automatic execution of any SPI-NT tools. This means all the tools must be executed manually by the operator. Additionally, the SPI-NT tools cannot be accessed through command-line interface. It is hoped that a future release of SPI for NT will allow for scheduled and/or unattended tool execution.

### 3.5.3 Reports.

The Report Manager Screen is accessed through Reports -> Manage Reports and provides the capability to view, print, archive, or delete reports. The Report Manager screen actually consists of two report listings: Incoming Reports and the Archive Reports. These lists are toggled with the `List Incoming` and `List Archives` buttons. Figure 3-3 shows a sample Report Manger screen displaying the Incoming Reports list. The list shows information about the report such as the job type, level, date/time started, and status of the job. The status for each job is checked when the Report Manager is started. When a new job is first entered into the system the STATUS is set to SUBMITTED. If the job is completed the STATUS will be COMPLETED. Note that the status will not change dynamically. The operator can leave the Report Manger and reenter to obtain the current job status.

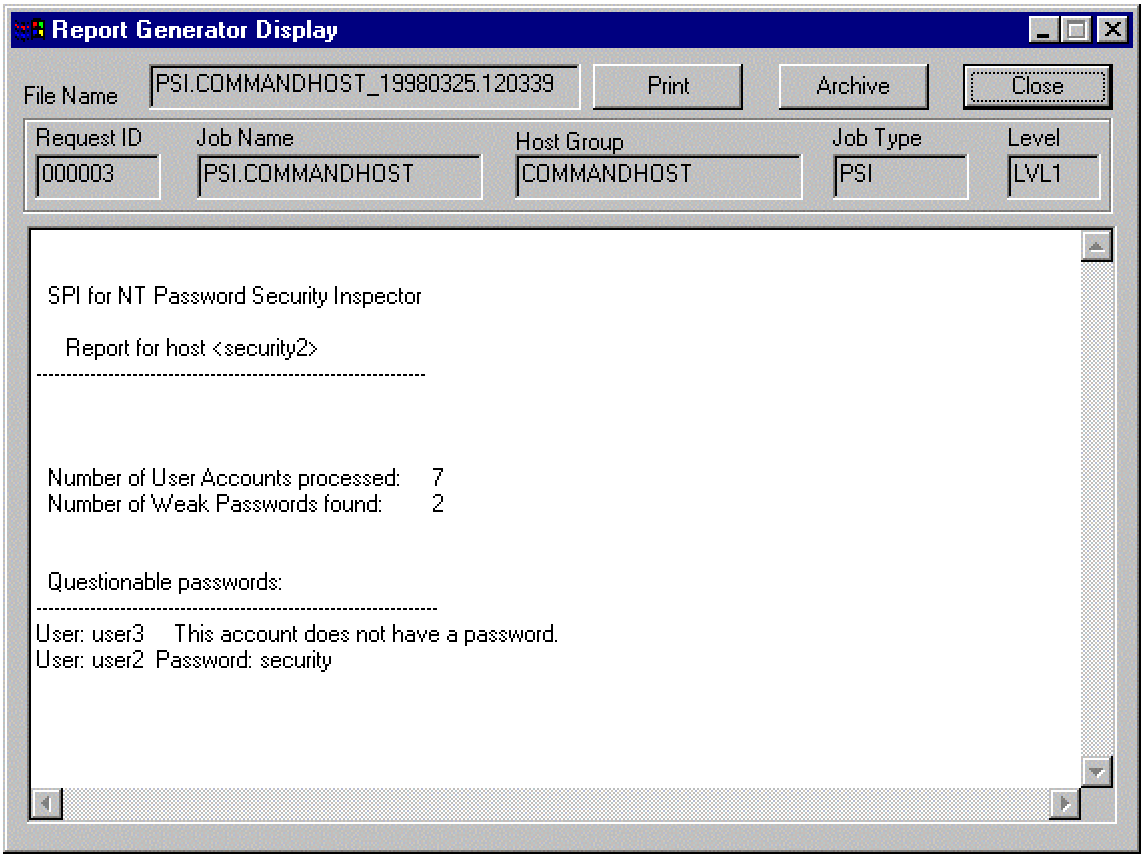


SPI for NT Incoming Report Listing

| Time | Job Name | Requester | Request ID | Job | Level | Host | Status |
|---|---|---|---|---|---|---|---|
| 19980325.114838 | BAT.COMMANDHOST | JOB OWNER | 000001 | BAT | LVL1 | COMMANDHOST | COMPLETED |
| 19980325.120309 | CDT.COMMANDHOST | JOB_OWNER | 000002 | CDT | LVL0 | COMMANDHOST | COMPLETED |
| 19980325.120339 | PSI.COMMANDHOST | JOB_OWNER | 000003 | PSI | LVL1 | COMMANDHOST | COMPLETED |
| 19980325.120734 | QSP.COMMANDHOST | JOB_OWNER | 000004 | QSP | LVL3 | COMMANDHOST | COMPLETED |

**Figure 3-3. Report Manager**

A report can be deleted from the Report Manager screen by selecting the `Delete` button or viewed by double clicking on the desired report. This action will cause the report to be displayed in the Report Generator Display (see Figure 3-4). The report can then be archived by selecting `Archive` or printed by pressing `Print`. The information in the Report Generator Display is similar to the Report Manager but also includes the filename associated with the job and report. Reports can be directly accessed via the directory area "…/SPI for NT 1.4/D/reps/*filename*."



File Name PSI.COMMANDHOST_19980325.120339

| Request ID | Job Name | Host Group | Job Type | Level |
|---|---|---|---|---|
| 000003 | PSI.COMMANDHOST | COMMANDHOST | PSI | LVL1 |

```
 SPI for NT Password Security Inspector

   Report for host <security2>
-----------------------------------------------------------------



 Number of User Accounts processed:    7
 Number of Weak Passwords found:       2


 Questionable passwords:
-------------------------------------------------------------------
User: user3    This account does not have a password.
User: user2  Password: security
```

**Figure 3-4. Report Generator Display**

3.6 Parameters and Configuration.
This section shows how to configure the various tools. To begin, this section examines the parameter files that are used to store SPI-NT tool configurations. SPI-NT uses two types of parameter template files: Pre-Loaded Templates and Machine Templates.

3.6.1 Pre-Loaded Templates.
This first type is a series of pre-loaded parameter template files included as part of the installation process. These templates are read-only and are intended to serve as a basis for developing user-define templates (Machine Templates). These templates could be considered "default" templates for tools that require little to no configuration.

The format for the pre-loaded templates is <*Tool*> <Level#>. Some examples are:

PSI Level1
QSP Level3

Note that Pre-loaded Templates do not contain or use any system extensions. Although they have the same elements as the template names, the actual filenames for templates are slightly different. The actual filenames for the above samples would be Psi_lvl1 and Qsp_lvl3 respectively. All template files are located in the directory areas associated with …/SPI for NT 1.4/D/parm/*Tool*/, where *Tool* is the common abbreviation for a particular tool.

### 3.6.2 Machine Templates.

Machine Templates are parameter templates associated with a specific system. Machine Templates are pre-loaded templates modified and saved for use by the operator. It is important to note that, in many circumstances, the default pre-loaded template must be modified to meet the requirements of the system. If this is not done then the usefulness of the SPI-NT tools are greatly diminished. It may seem unusual for SPI-NT to use machine names or system references when it is a single host application. However, the UNIX version of Security Profile Inspector (SPI) is a multi-host application with remote execution capabilities. Most likely, a future release of SPI for NT will have multi-host capability. The format for the Machine Templates is the same as the Pre-loaded Templates except a machine or system extension is used.

Samples of the format are:

PSI Level1 security2
QSP Level3 security2

In these samples "security2" is the name associated with the Windows NT machine. The actual filenames associated with the Machine Templates, like those with the Pre-loaded Templates, use a slightly different format. For the samples above, the actual filenames would be PSI_LVL1.HID_000001 and QSP_LVL3.HID_000001. The HID_000001 extension relates to the UNIX version of SPI and is the default designation for the primary host in a multi-host system.

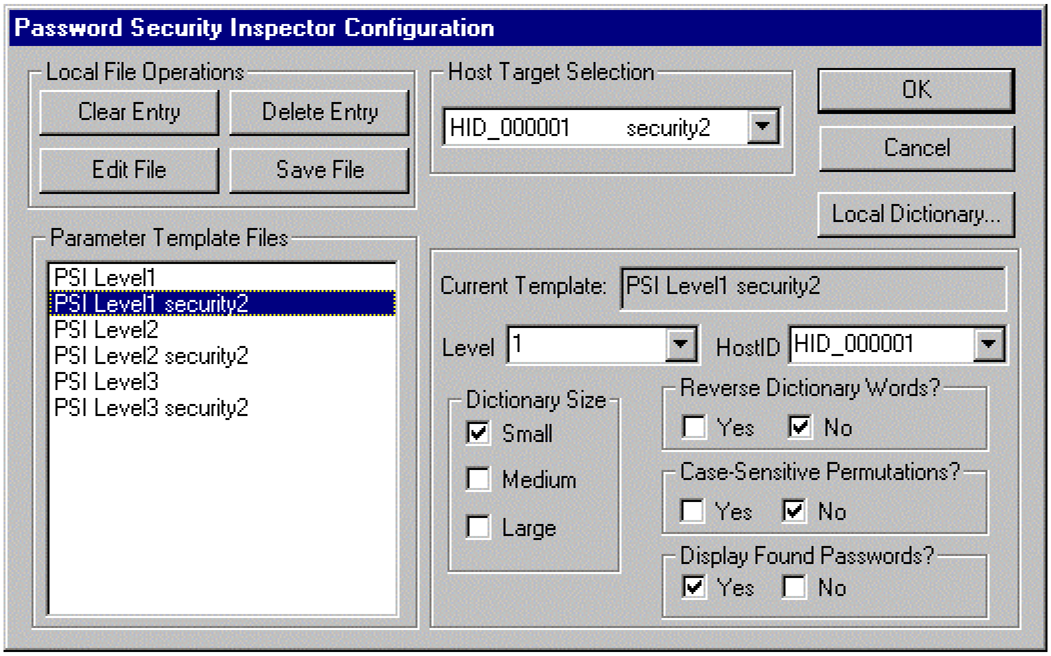
### 3.6.3 Configuration Levels.

Levels are used to allow the operator to have various levels of intensity or scrutiny. Generally, each tool has three configuration levels, numbered 1, 2, and 3. By default, Level 1 is the least intense and Level 3 is the most intense. However, the operator can adjust these levels and associated parameter templates to perform whatever tasks are desired. Though most tools have three levels, there are a couple of exceptions to this for the Change Detection Test (CDT) and the Binary Authentication Tool (BAT). For the CDT, a Level 0 is used to create baseline filesystem snapshots. The BAT only has a single configuration level which is not adjustable by the user. The need for these adaptations will become apparent in the discussion of the tool configuration procedures.

### 3.6.4 Generic Configuration Procedures.

To begin the tool configuration process, select the desired tool in the Jobs menu. At the job window (see Figure 3-1) select `Configure` to bring up the tool configuration window. A sample tool configuration window for a Password Security Inspector (PSI) configuration is shown in Figure 3-5. The basic layout of all tool configuration screens is essentially the same.

The lower-left portion of the window is the `Parameter Template Files` area, which contains a listing of both Pre-loaded and Machine Templates associated with a particular SPI-NT tool. The upper-left portion of the screen is the `Local File Operations` area. Use the buttons in this area to Clear, Delete, Edit, or Save a parameter template file. The upper-right portion of the window is the `Host Target Selection` area. This identifies the host with which the Parameter Template is associated. This area is not actively used because SPI for NT is a single host application. Lastly, the lower-right portion is the tool-unique configuration area. This area, in addition to having tool-unique parameter designation entries, also contains the Current Template filename, the Level and HostID for the template currently being viewed and/or modified. Once again the HostID entry is not actively used.



Password Security Inspector Configuration

Host Target Selection: HID_000001 security2

Parameter Template Files:
PSI Level1
PSI Level1 security2
PSI Level2
PSI Level2 security2
PSI Level3
PSI Level3 security2

Current Template: PSI Level1 security2

Level 1 HostID HID_000001

Dictionary Size
☑ Small
☐ Medium
☐ Large

Reverse Dictionary Words?
☐ Yes ☑ No

Case-Sensitive Permutations?
☐ Yes ☑ No

Display Found Passwords?
☑ Yes ☐ No

**Figure 3-5. Tool Configuration Window**

With the tool configuration window displayed, the first step is to select a file from the `Parameter Template Files` area that is to be modified or used as the basis for a new configuration template. To edit the parameter file, either double-click the file entry or select a file and press the `Edit File` button. To modify an existing file, adjust the tool specific configuration parameters and press the `Save File` button to store the changes. If the selected template is being used as a basis for a new parameter template, adjust the Level as desired, make any tool-specific modifications, then press the `Save File` button. A new Parameter Template File should be created and displayed in the Parameter Template Files area.

### 3.7 Tools Specific Configuration Details.

This section examines the details for each specific tool.

### 3.7.1 Binary Authentication Tool (BAT).

Description. The BAT performs several crucial checks of the Windows NT 4.0 operating system. First, the tool checks to see if any Service Packs (SP), through SP3, need to be applied. In addition to this, BAT will report if files are missing or do not match the binary checksums for the Windows NT systems files. The binary authentication table is provided as part of the SPI-NT installation and will check the system binaries against the original distribution through Service Pack 3. The table includes the filename and the MD5 checksum value for all systems files. An entry that cannot be identified through a checksum could possibly be a Trojaned dynamic link library (DLL) or system binary file and will be identified as such.

Configuration. Since BAT checks the system files for existence and proper checksum, there are no configuration parameters for the BAT utility.

Sample Report. The following is a sample report that highlights the form and sample findings available using the BAT tool. Note that the report has been edited for space and contents.

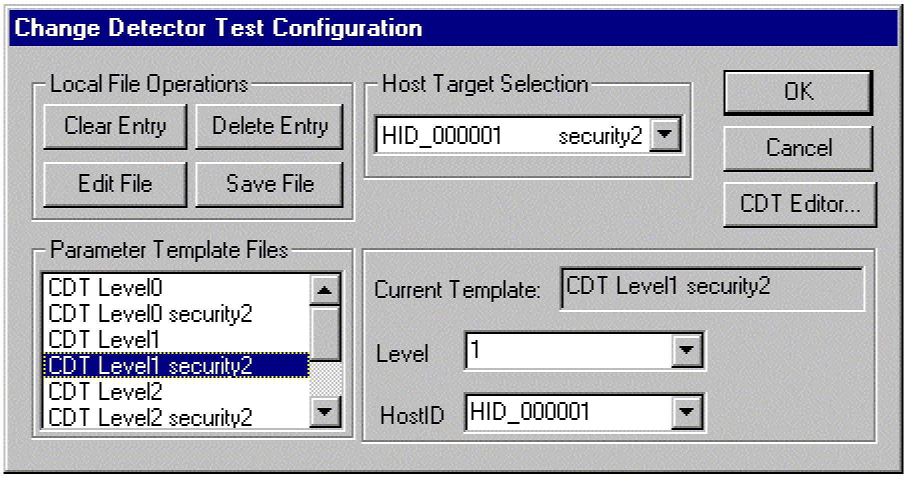
```
  SPI for NT Binary Authentication Tool

    Report for host <security2>
-----------------------------------------------------------------


    Obsolete Binaries Found

C:\WINNT\system32\acledit.dll
  Original Distribution:  Should be patched with Service Pack 3.

C:\WINNT\system32\advapi32.dll
  System patched with Service Pack 2:  Should be patched with Service Pack 3.

C:\WINNT\system32\lsasrv.dll
  System patched with Service Pack 2:  A Hotfix is available for this binary.
  (See Microsoft's web site http://www.microsoft.com/security/ for hotfixes.)

    Unrecognized Binaries Found

C:\WINNT\inf\intl.inf

  Current Check Sum
    694AC7567FA5C47863280EC8B8C01FA8
  Authentication Check Sum
    54815E0CE40BCF7CFFF2C4D8CF6C97ED
```

```
   Missing Binaries Reported

C:\WINNT\inf\splayout.inf
C:\WINNT\system32\asycfilt.dll
C:\WINNT\system32\chkntfs.exe
C:\WINNT\system32\dllhost.exe
C:\WINNT\system32\drivers\el59x.sys
C:\WINNT\system32\drivers\rasarp.sys
```

### 3.7.2 Change Detector Test (CDT).

Description. The CDT is a tool that will report changes to a set of user-selected files by performing a before and after comparison of the file set. The before picture is a Level 0 inspection which creates a baseline snapshot of the user selected files. Subsequent inspections using Levels 1-3 are compared against this baseline to detect changes to the file set. Note that a Level 0 must be performed before a Level 1-3 inspection can be performed. CDT will check for files that have been added, deleted, or modified. Additionally, CDT can check file attributes such as the owner, file size, MD5 checksum, checksum length, permissions, file mode, creation time, modify time, change time, and access time as directed by the operator. Through proper utilization, the operator has a host level intrusion detection tool that can detect changes to files and their attributes. This is particularly useful when applied to system binaries, DLLs, applications binaries and other “static” files.

Configuration. The configuration of the CDT consists of the selection of files to be placed under observation and the determination of which attributes will be monitored. Figure 3-6 shows the Change Detector Configuration window. Unlike most of the other SPI-NT tools, the actual configuration takes place in a separate window called the CDT Editor that is accessed by pressing the corresponding button. Proper configuration procedures would be to first select an appropriate template file, then click on either the `CDT Editor` button or the `Edit File` button.



Change Detector Test Configuration

Host Target Selection: HID_000001 security2

Parameter Template Files:
CDT Level0
CDT Level0 security2
CDT Level1
CDT Level1 security2
CDT Level2
CDT Level2 security2

Current Template: CDT Level1 security2

Level: 1

HostID: HID_000001

**Figure 3-6. CDT Parameter Window**

The CDT Editor screen, as shown in Figure 3-7, is where the operator selects which files and file attributes are to be monitored. The operator creates a series of inspection entries that consist of a file or directory, any Include Filter, any Exclude Filter, and warning specifications. The basic steps for establishing a file monitoring criteria are listed below:

(1) Select the file or directory from the System Files area. This area will show those drives on the system that utilize the NTFS file system. (CDT does not operate on non-NTFS disks.) These drives can be expanded by double clicking on the drive entry. Directories will be indicated by a square box containing a plus (+) sign. The boxes can be expanded by double clicking on the directory entry.

(2) Determine any possible Include Filters or Exclude Filters. Include Filters removes the tedium of having to create entries for each file to be monitored. By using an Include Filter, wildcards can be used to select multiple files in a directory area. The most common Include Filter is the "*" which will include all files in that directory. Note that Include Filters are not recursive and will not include any files located in sub-directories of a given directory. Exclude Filters are used in conjunction with Include Filters to remove particular files from being included in the inspection as part of the Include Filter process. This allows for further refinement of the filter process. The Include Filter and Exclude Filter are applied only when the corresponding On box has been checked. For file entries these boxes must be unchecked or the entry will not be accepted by the system.

(3) Determine Warning Specifications to be utilized for this file/directory entry. After the file(s) have been selected, the operator selects which file attributes, if any, will be monitored by the CDT. The available attributes are:

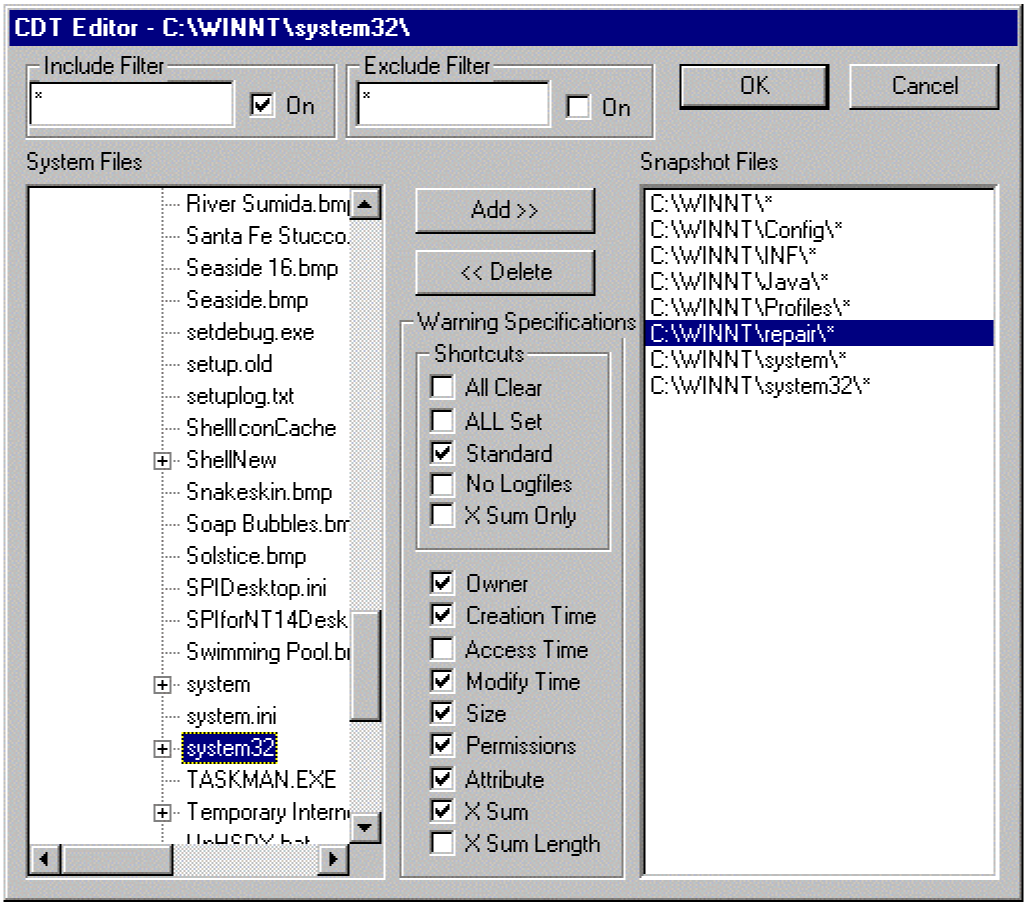
- Owner
- Access Time
- Creation Time
- Modify Time

- Size
- X Sum (MD5 Checksum)
- Attributes (archive, read-only, hidden, system)
- Permissions (NT access control list)
- X Sum Length

Several shortcuts allow quick use of pre-set warning specification templates:

- All Clear - No items selected
- All Set - All items selected
- Standard - Owner, Creation Time, Modify Time, Size, Permissions, Attribute, X Sum
- No Logfiles - Owner, Permissions, Attribute
- X Sum Only - X Sum, X Sum Length

(4) Add Entry. Select the `Add>>` button to add this entry to the Snapshot Files area. Entries already in the Snapshot Files area can be viewed by selecting that entry and can be removed by pressing the `<<Delete` button.



Include Filter: * ☑ On

Exclude Filter: * □ On

System Files:

River Sumida.bm
Santa Fe Stucco.
Seaside 16.bmp
Seaside.bmp
setdebug.exe
setup.old
setuplog.txt
ShellIconCache
ShellNew
Snakeskin.bmp
Soap Bubbles.bm
Solstice.bmp
SPIDesktop.ini
SPIforNT14Desk
Swimming Pool.b
system
system.ini
system32
TASKMAN.EXE
Temporary Intern

Snapshot Files:

C:\WINNT\*
C:\WINNT\Config\*
C:\WINNT\INF\*
C:\WINNT\Java\*
C:\WINNT\Profiles\*
C:\WINNT\repair\*
C:\WINNT\system\*
C:\WINNT\system32\*

Warning Specifications

Shortcuts
□ All Clear
□ ALL Set
☑ Standard
□ No Logfiles
□ X Sum Only

☑ Owner
☑ Creation Time
□ Access Time
☑ Modify Time
☑ Size
☑ Permissions
☑ Attribute
☑ X Sum
□ X Sum Length

**Figure 3-7. CDT Editor**

Operating Notes.

(1) All CDT Pre-loaded Templates utilize all of the Warning Specification file attributes against the files located in the directory from which Windows NT is executed. Normally this will be the directory C:\WINNT.

(2) Once a CDT parameter template has been created and saved, on subsequent editing sessions, the CDT Editor will not properly display the file elements and attribute settings. In fact nothing will be shown. This is a known glitch in the software. The CDT Editor currently being used is slated to be replaced in a future release. However, the operator can use the Notepad or other text editors to view CDT parameter files which are located in …/SPI for NT 1.4/D/parm/cdt. The format used is similar to that used by SPI-NET. See Appendix A: Change Detection Test (CDT) Parameter File Basics for information on reading and understanding the CDT parameter file.

Sample Report. The following sample report highlights the form and sample findings available using the CDT tool. Note that the report has been edited for space and content.

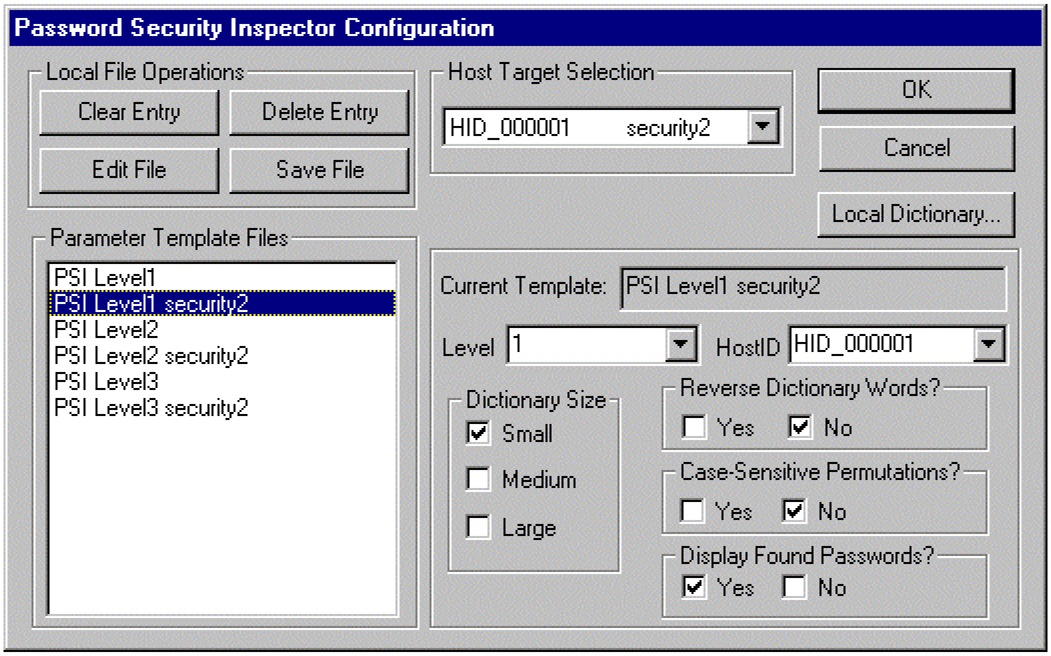
```
SPI for NT Change Detection Test

    Report for host <security2>
----------------------------------------------------------------
  Files that have changed:

    C:\WINNT\ACT.ini
  Access Time:
  new 19980325.152535
  old 19980325.114556

    C:\WINNT\TASKMAN.EXE
  Access Time:
  new 19980325.154817
  old 19980325.114838

    C:\WINNT\TASKMAN.EXE
    SACL ACE ("Everyone" "0x001f01ff")  was deleted

    C:\WINNT\TASKMAN.EXE
    SACL ACE ("Administrators" "0x001f01ff")  was added

  Files that were added:
```

```
  C:\WINNT\Notepad.exe

 Files that were deleted:

  C:\WINNT\NOTEPAD.EXE
  C:\WINNT\REGEDIT.EXE

Summary Information
Total Added:  1
Total Changed:  76
Total Deleted:  2
```

### 3.7.3 Password Security Inspector (PSI).

Description. PSI attempts to find weak passwords in local user accounts with dictionary based attacks and permutations based on the user name. PSI uses two primary methods to discover weak passwords. One is a modified "Joe account" algorithm that starts by checking the user name as the password and then proceeds to insert special characters between each of the letters of the user name. The second method uses dictionary attacks to check for weak passwords.

Configuration. As shown in Figure 3-8, four configuration options are available along with the ability to create and use a localized or operator defined dictionary. These options are explained below:



Password Security Inspector Configuration

Host Target Selection: HID_000001 security2

Parameter Template Files:
PSI Level1
PSI Level1 security2
PSI Level2
PSI Level2 security2
PSI Level3
PSI Level3 security2

Current Template: PSI Level1 security2

Level 1 HostID HID_000001

Dictionary Size: ☑ Small □ Medium □ Large

Reverse Dictionary Words? □ Yes ☑ No

Case-Sensitive Permutations? □ Yes ☑ No

Display Found Passwords? ☑ Yes □ No

**Figure 3-8. PSI Configuration Window**

Dictionary Size (Small/Medium/Large). SPI-NT comes installed with three pre-generated dictionaries of different sizes: Small, medium and large. One of these dictionaries must be utilized as part of the password cracking process. In addition to the dictionary selected, the Local Dictionary, which the operator defines, will be utilized. Modifications to the Local Dictionary can be made by pressing the `Local Dictionary` button. The larger the dictionary used, the more intense the password checking will be, and the longer it will take to complete.

Reverse Dictionary Words? (Yes/No). By enabling this option, the password checking routine will also use the reverse of the dictionary words in addition to the dictionary word. For example, if one of the dictionary words is “bat” and the option is enabled, then PSI will check for both “bat” and “tab.”

Case-Sensitive Permutations? (Yes/No). If this option is selected, PSI will check all case-sensitive permutations of all dictionary words. For example, if the dictionary word was “it,” PSI would check for “it,” “IT,” “It,” and “iT.”

Display Found Passwords? (Yes/No). If this option is enabled, the password of any accounts that have been cracked will be printed in the report. Since this information is highly sensitive, usage of this option should be carefully reviewed. If the option is used, check access to the report files and the SPI-NT program and secure any hard copy reports.

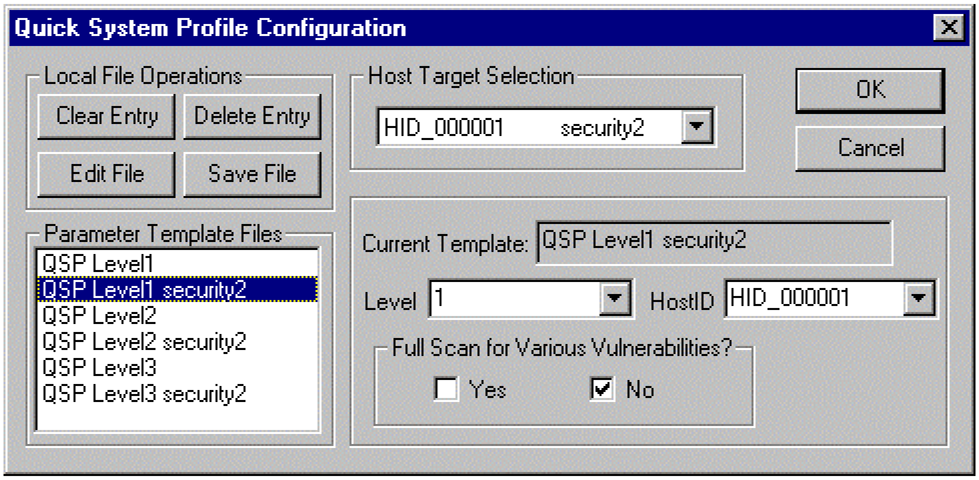
Sample Report. The following is a sample report that highlights the form and sample findings available using the PSI tool. Note that the report has been edited for space and content.

```
 SPI for NT Password Security Inspector

   Report for host <security2>
---------------------------------------------------------------

 Number of User Accounts processed:    7
 Number of Weak Passwords found:       2

 Questionable passwords:
-----------------------------------------------------------------
User: user3      This account does not have a password.
User: user2  Password: security
```

### 3.7.4 Quick System Profile (QSP).

Description. QSP performs a series of standardized checks to detect vulnerabilities. It checks for permissions on system files and DLLs, proper implementation of NT Registry Keys, and weak passwords in Administrator and Guest accounts.

Configuration. There is only one option available for QSP. As shown in Figure 3-9, this option enables or disables the Full Scan for Various Vulnerabilities which performs an in-depth inspection of access permissions to DLLs in windows and system directories.



Host Target Selection: HID_000001 security2

Parameter Template Files:
QSP Level1
QSP Level1 security2
QSP Level2
QSP Level2 security2
QSP Level3
QSP Level3 security2

Current Template: QSP Level1 security2

Level 1 HostID HID_000001

Full Scan for Various Vulnerabilities?
☐ Yes ☑ No

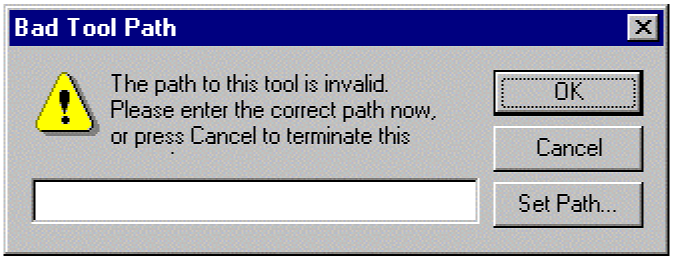
**Figure 3-9. QSP Configuration Window**

Sample Report. The following is a sample report that highlights the form and sample findings available using the QSP tool. Note that the report has been edited for space and content.

```
 SPI for NT Quick System Profile

   Report for host <security2>
---------------------------------------------------------------

  Warning: Everyone has Change permissions to:
C:\WINNT\System32\ACTXPRXY.DLL

  Warning: Everyone has Change permissions to:
C:\WINNT\System32\WSOCK32N.DLL

  Error: Administrators have Full permissions to:
C:\WINNT\repair\sam._
Exploitation may allow remote users to gain Administrator privileges.
CIAC Bulletin:  http://ciac.llnl.gov/ciac/bulletins/h-45.shtml

  Error: Everyone has Read permissions to:
C:\WINNT\repair\sam._
Exploitation may allow remote users to gain Administrator privileges.
CIAC Bulletin:  http://ciac.llnl.gov/ciac/bulletins/h-45.shtml

  Warning: Administrator Account "Administrator" has not been renamed.

  Warning: Value-pair DontDisplayLastUserName at registry key
System\CurrentControlSet\Control\Lsa does not exist.
The user name of the last user to log on the computer
is displayed in the User name text box of the Logon dialog box.
An intruder with access to the Logon dialog can use that
account to break into the system.
```

3.7.5 Virus Detector Tool (VDT).

SPI for NT has provisions to allow the operator to link a user provided VDT into the SPI-NT system. On the first launch of the VDT, the operator will be prompted for the location of the virus detector. This is shown in Figure 3-10. Enter the full path to the virus detector and select Set Path to initially go to the virus detector. Click `Yes` at the Confirm Save Tool Path prompt to save the path for future use.



The path to this tool is invalid.
Please enter the correct path now,
or press Cancel to terminate this

**Figure 3-10. VDT Path Entry Screen**

3.8 Operating Recommendation.

To obtain the full security benefits from SPI for NT, the tools must be run on a regular basis. Since SPI-NT does not currently provide a scheduling mechanism, the burden of tool scheduling and execution is solely on the operator. The following are some general guidelines that may help the operator in scheduling and executing the SPI-NT tools.

| Tool | Frequency |
|---|---|
| Binary Authentication Tool (BAT) | Weekly |
| Change Detection Test (CDT) | Daily |
| Password Security Inspector (PSI) | Daily |
| Quick System Profile (QSP) | Weekly |

Usage of the tools should be adapted to suit the system on which they are being run. A heavily used system with many users may need to run the tools more frequently than stated. Additionally, running the tools is little use if the reports are not also reviewed by the operator or system administrator.

## Appendix A: Change Detection Test (CDT) Parameter File Basics

The basic parameter file used by the CDT is simple to understand if the operator knows how to read it. The MetaSpec, or parameter file, used by the CDT is essentially a text file made up of MetaSpec line entries. Each entry has three required fields and an optional field as shown below:

**“Type”: “WarnSpec”: “Target”: ““[Exceptions]””**

A sample CDT parameter file might look like:

```
“FILE”: “acpmstuxr”: “C:\AUTOEXEC.BAT”: ““””
“FILE”: “acpmstuxr”: “C:\CONFIG.SYS”: ““””
“FILE”: “cpmsuxr”: “C:\WINNT\*.ini”: ““infoview.*””
“FILE”: “cpmsuxr”: “C:\WINNT\*.exe”: ““””
```

*Type* indicates what type of object is being examined. For SPI-NT the type will always be FILE. A File type is used to identify file and directory items that are to be monitored for change. For other versions of SPI, the types User and Group are also allowable. The User and Group types identify the users or groups to be monitored.

*WarnSpec* (Warning Specification) defines the change detection attributes to be activated. Each warning specification will have a letter identifier to represent that specification. For the type FILE, the allowable change detection attributes are:

| | |
|---|---|
| (u) | Owner |
| (c) | Creation Time |
| (a) | Access Time |
| (m) | Modify Time |
| (s) | Size |
| (p) | Permissions |
| (x) | Xsum (Checksum) |
| (t) | Xsum Length (Checksum Length) |

*Target* indicates the file to be examined for possible changes. The File type can use standard UNIX wildcards to help define files and directories for monitoring. These wildcard specifications are implemented through the Include Filter.

*Exceptions* allow the user to omit particular files from the defined Target. Since wildcards are allowed in the Target specifications, the Exceptions area allows the operator to omit specific files from a wildcard inclusion.

Looking at the sample parameter file above, the four entries are explained below:

“FILE”: “acpmstuxr”: “C:\AUTOEXEC.BAT”: “‘’”

> This entry checks the file C:\AUTOEXEC.BAT. All of the warning specifications are selected. These are (a) Access Time; (c) Creation Time; (p) Permissions; (m) Modify Time; (s) Size; (t) X Sum Length; (u) Owner; (x) X Sum or Checksum; and (r) Attributes.

“FILE”: “acpmstuxr”: “C:\CONFIG.SYS”: “‘’”

> This entry checks the file C:\CONFIG.SYS. All of the warning specifications are selected. These are (a) Access Time; (c) Creation Time; (p) Permissions; (m) Modify Time; (s) Size; (t) X Sum Length; (u) Owner; (x) X Sum or Checksum; and (r) Attributes.

“FILE”: “cpmsuxr”: “C:\WINNT\*.ini”: “‘infoview.*’”

> This entry checks for all files located in the C:\WINNT| directory that have the extension “.ini.” The exclusion field of infoview.* will prevent the file infoview.ini from being included in file checks. The standard shortcut was used to indicate the warning specifications. These are (c) Creation Time; (p) Permissions; (m) Modify Time; (s) Size; (u) Owner; (x) X Sum or Checksum; and (r) Attributes.

“FILE”: “cpmsuxr”: “C:\WINNT\*.exe”: “‘’”

> This entry checks for all the files located in the C:\WINNT| directory that have the extension “.exe”. The Standard shortcut was used to indicate the warning specifications. These are (c) Creation Time; (p) Permissions; (m) Modify Time; (s) Size; (u) Owner; (x) X Sum or Checksum; and (r) Attributes.